UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

United States of America

v.

Report and Recommendation
15-CR-159W

Daniel G. Sasiadek,

Defendant.

I. INTRODUCTION

Defendant Daniel Sasiadek ("Sasiadek") allegedly visited an anonymous Internet site to view and to download child pornography. When Federal Bureau of Investigation ("FBI") agents took over the Internet site, they wanted to find out who had been logging in and visiting the site. To accomplish that goal, FBI agents received permission from a Magistrate Judge in the Eastern District of Virginia to plant monitoring software on any computer that connected with the Internet site's server. The monitoring software would transmit information that would allow the agents to identify the user at the computer. In this way, FBI agents eventually discovered that Sasiadek was one of the Internet site's visitors. From there, FBI agents obtained a search warrant from this Court for Sasiadek's residence. Upon executing the search, the FBI agents found child pornography in Sasiadek's possession; the Government since has charged him accordingly.

Sasiadek now has filed motions to suppress any evidence that traces back to the use of the monitoring software to discover his identity. (Dkt. No. 30 at 3; Dkt. No. 87.) Among other arguments, Sasiadek argues that the Magistrate Judge from the Eastern District of Virginia lacked authority to authorize the broad type of search that occurred here and any type of search outside of

her own district. Sasiadek also disputes some of the information presented to that Magistrate Judge and raises policy concerns about how the FBI set itself up to capture information about visitors to the Internet site. The Government opposes suppression, arguing that the warrant in question was proper, that the effort required to reach the Internet site by itself supports probable cause, and that the FBI agents relied on the warrant in question in good faith.

The Hon. Elizabeth A. Wolford has referred this case to this Court under 28 U.S.C. § 636(b). (Dkt. No. 14.) The Court held oral argument on April 19 and October 12, 2017. For the reasons below, the Court respectfully recommends denying Sasiadek's motions.

II. BACKGROUND

This case concerns allegations that Sasiadek possessed child pornography on multiple electronic devices and attempted to use a minor to produce child pornography. The final events leading to Sasiadek's arrest are not in dispute and resemble other cases involving child pornography. In 2015, FBI agents identified an Internet Protocol ("IP") address that connected with an Internet site named "Playpen." Playpen was known to harbor child pornography; some content apparently would not meet the statutory criteria for child pornography, but the parties do not dispute that most content on the site would. Playpen was not accessible via the World Wide Web; as a "hidden service" or "dark web" site, Playpen was accessible only by way of a network known as The Onion Router, or "Tor."[1] After contacting the Internet service provider Time Warner Cable, FBI agents confirmed that the IP address in question belonged to Sasiadek. Once FBI agents confirmed Sasiadek's IP address and residential address, they submitted an application

[1] A brief description of how the Tor network and browser operate appears in a hearing transcript that now is part of this record. (*See* Dkt. No. 42 at 100–02.)

to this Court for a search warrant for Sasiadek's residence. (Dkt. No. 42 at 8; *see generally* Case No. 15-MJ-2113.) The Court issued the search warrant on July 16, 2015.[2]

Proceedings in this case began shortly after the Court issued its search warrant. FBI agents searched Sasiadek's residence and arrested Sasiadek on July 17, 2015, and the Government filed a pre-indictment complaint on the same day. (Dkt. No. 1.) The Court held an initial appearance on July 17, 2015 and a detention hearing on July 22, 2015. Sasiadek has been in continuous custody since his arrest. The most current accusatory instrument is the superseding indictment that the Government filed on May 5, 2016. (Dkt. No. 19.) The superseding indictment contains eight counts plus a forfeiture notice. In Count One, the Government accuses Sasiadek of production of child pornography in violation of 18 U.S.C. §§ 2251(a) and 2251(e). In Counts Two through Eight, the Government accuses Sasiadek of possession of child pornography on different electronic media, in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and 2252A(b)(2). The forfeiture notice pertains to the various electronic media seized from Sasiadek's house that allegedly contain child pornography.

The above details are not unusual for a case like Sasiadek's. What makes this case unusual is how FBI agents obtained Sasiadek's IP address in the first place. Playpen, being a hidden service within the Tor network, did not collect or store the IP addresses of its visitors. Playpen also encouraged visitors to log in anonymously using fictitious names and email addresses. (*See, e.g.*, Dkt. No. 42 at 69 (reposting Playpen disclaimer to users warning them not to enter a real email

[2] The search warrant lists the date of July 17, 2015, but July 16 likely was intended as this latter date matches the dates in the application. This clerical discrepancy does not appear to affect any of the issues in the case, but the Court notes it for the sake of the record.

address).) Consequently, when FBI agents took over Playpen in February 2015,[3] they had no way of knowing who was visiting the site, how frequently anyone visited the site, or what visitors did once they entered the site. To defeat Playpen's anonymity, FBI agents employed a tactic called a Network Investigative Technique ("NIT"). The NIT consisted of software—Sasiadek and at least some courts have used the pejorative term malware—that bypassed any defenses on a Playpen visitor's computer and installed itself surreptitiously. The NIT installed itself as soon a visitor logged in and reached the landing page; installation did not require any confirmed downloads of child pornography. No computer could pick up the NIT without first visiting the Playpen site. Once installed, the NIT executed one function: obtain the IP address and other identifying information for the computer that contacted the Playpen site, and transmit that information to the FBI.

FBI agents obtained permission to set up and to execute the NIT from a single Magistrate Judge in the Eastern District of Virginia. In the warrant application, the agents described the place to be searched as a combination of the Playpen server, "located at a government facility in the Eastern District of Virginia" (Dkt. No. 42 at 54), and the computers "of any user or administrator who logs into [Playpen] by entering a username and password." (*Id.*) The agents described the information that they sought through the NIT, including any given computer's IP address, operating system, host name, operating system username, and media access control ("MAC")

[3] While not directly relevant to any of the issues in this case, the Court briefly will note the back story leading to the FBI investigation. In short, Stephen Chase created Playpen in August 2014. The site might well have remained anonymous to this day except that Chase accidentally exposed Playpen's IP address, leading international law enforcement agents to trace the Playpen server to Florida. *See, e.g.*, Narjas Zatat, *Police Arrest 870 Suspected Paedophiles and Rescue Hundreds of Children after Smashing International Internet Ring*, UK Independent, May 7, 2017 (available in LexisNexis).

address, along with a unique identifier that the software itself would generate. (*Id.* at 55.) The agents described Playpen as "dedicated to the advertisement and distribution of child pornography, the discussion of matters pertinent to child sexual abuse, including methods and tactics offenders use to abuse children, as well as methods and tactics offenders use to avoid law enforcement detection while perpetrating online child sexual exploitation crimes such as those described in paragraph 4 of this affidavit." (*Id.* at 65.) Another section of the application describes playpen as a site that "appeared to be a message board website whose primary purpose is the advertisement and distribution of child pornography." (*Id.* at 68.) With respect to the NIT software itself, the FBI agents describe the software as "additional computer instructions" that would "cause" a computer "to transmit certain information to a computer controlled by or known to the government." (*Id.* at 79.) The agents did not describe how the "instructions" would download surreptitiously and would bypass all antivirus and malware defenses on the computer. The agents did, however, put the Magistrate Judge on notice that the NIT would operate on affected computers "wherever located." (*Id.* at 84.) The Magistrate Judge approved the application and issued the search warrant on February 20, 2015.

On September 28, 2016, Sasiadek filed a motion to suppress all evidence obtained with the help of the NIT. (Dkt. No. 30 at 3; Dkt. No. 87.) Sasiadek seeks suppression for several reasons. Sasiadek argues that the Magistrate Judge in the Eastern District of Virginia wound up issuing a warrant that authorized a search outside of her district, thereby violating the territorial limits of Rule 41(b) of the Federal Rules of Criminal Procedure. A similar argument advanced by Sasiadek is that the NIT warrant did not authorize the search of his computer in this District. The NIT

warrant additionally "did not (because it could not) specify who these users were or where their computers could be located. The warrant therefore failed to particularly describe the computers to be searched in violation of the Fourth Amendment." (*Id.*) Sasiadek also challenges the probable cause finding behind the NIT warrant and the information that FBI agents provided to the Magistrate Judge. The agent who applied for the NIT warrant told the Magistrate Judge "that 'the entirety' of Playpen is 'dedicated to child pornography,' and described the site as a 'website whose primary purpose is the advertisement and distribution of child pornography.'" (Dkt. No. 40 at 3; *see also* Dkt. No. 42 at 75.) Sasiadek disputes this characterization as intentionally misleading and counters that the website had a mix of legal and illegal content that would not be obvious from the landing page within the site that would trigger installation of the NIT. (*See also id.* at 9 ("Because the NIT warrant application contained no specific information about the site's visitors and the application did not include an expert 'collector profile,' probable cause depended on the contents of the home page and whether it was likely that anyone who saw that page would know that its contents were illegal before proceeding to actually take a look.") (citation omitted); Dkt. No. 42 at 70–72 (listing of landing page contents).) On a broader policy level, Sasiadek takes issue with how, in his view, the FBI essentially became a child pornography distributor for two weeks to defeat Playpen's anonymity:

> To ensnare its targets, the FBI maintained and operated Playpen from February 20, 2015 until at least March 4, 2015. During this time the FBI ran Playpen just as the prior management, allowing new users to sign up, members to post child pornography, and any registered visitor to view and download illegal materials. It made no effort to block or limit the uploading, downloading, viewing, or redistribution of countless illegal pictures and videos. In fact, site traffic actually increased while Playpen was under the FBI's stewardship. As of February 20, 2015

> the site had 158,094 members and enjoyed approximately 11,000 weekly visitors. According to government information, approximately 56,000 new members joined the site after the FBI took it over and about 100,000 users visited the site during the two-week period that the FBI operated it, a dramatic improvement over the site's performance under pre-FBI management.

(Dkt. No. 40 at 7.)

The Government opposes Sasiadek's motion in all respects. The Government begins with a factual dispute over Sasiadek's insinuation that the FBI effectively became a child pornography distributor in 2015. The Government specifically disputes Sasiadek's assertion that new users joined Playpen while the site was under FBI control:

> Once a user accepted those terms and conditions, a user was required to enter a username, password, and e-mail address. Upon successful registration, all of the sections, forums, and sub-forums, along with the corresponding number of topics and posts in each, were observable. Significantly, the NIT would *only* gather IP address information on registered users of Playpen—that is—those users who had *already signed up for an account* with the child pornography website before the FBI's involvement. If a new user visited Playpen while it was under FBI control, they would not be able to register, and thus would not be able to access any of the website's content.

(Dkt. No. 43 at 5.) The Government does not necessarily dispute Sasiadek's contention that Playpen's landing page itself does not contain illegal content. Instead, the Government emphasizes how Playpen's index on the landing page contains links to folders whose names signaled the presence of illegal content. From there, the Government argues that the effort required to access Playpen by itself supported a finding of probable cause. Based on the anonymity of the site, the need to use the Tor network to reach the site, and the registration requirements, the Government argues that anyone who went through that effort knew that the site contained child pornography and proceeded through the site for that reason. The presence or absence of

illegal content right on the landing page thus was unnecessary. (*See* Dkt. No. 43 at 16.) With respect to particularity, the Government emphasizes that the NIT deployed only on computers that reached the Playpen site, not computers generally, and that it deployed only when those computers electronically entered the Eastern District of Virginia by connecting with Playpen's server. This latter point, according to the Government, made the NIT similar to a tracking device whose installation had been authorized in the Eastern District of Virginia. Finally, even if a constitutional violation or a violation of Rule 41 occurred, the Government nonetheless urges denial of suppression under the good-faith principle established by *United States v. Leon*, 468 U.S. 897, 922 (1984). Under the good-faith principle, the Government argues that the FBI agents did not intentionally mislead the Magistrate Judge and did not mislead her in any material way. As a result, any error in issuing the NIT warrant was the error of the Magistrate Judge and not the error of the FBI agents. Suppression of evidence under these circumstances, in the Government's view, would not serve the purpose of the exclusionary rule because the FBI agents committed no misconduct that would need to be deterred.

III. DISCUSSION

The parties have done a commendable job researching a number of constitutional and statutory issues related to the NIT. These issues have arisen because of the unusual way in which the NIT works. The NIT has elements of a tracking device; like a tracking device, the NIT downloads or installs in one place but can deliver information about a person wherever that person goes. The NIT has elements of an anticipatory search warrant; like an anticipatory search warrant, the NIT installs itself before actual illegality occurs but under circumstances that suggest

that illegality is imminent. *See, e.g., United States v. Grubbs*, 547 U.S. 90, 96–97 (2006) ("In other words, for a conditioned anticipatory warrant to comply with the Fourth Amendment's requirement of probable cause, two prerequisites of probability must be satisfied. It must be true not only that *if* the triggering condition occurs there is a fair probability that contraband or evidence of a crime will be found in a particular place, but also that there is probable cause to believe the triggering condition *will occur*.") (internal quotation marks and citations omitted). Finally, the NIT does have some elements of the traditional search warrant and the issues that accompany those warrants. For example, in a drug case, if surveillance, call intercepts, and controlled purchases led law enforcement agents to believe that drug transactions were occurring at a particular house then, under the right circumstances, probable cause would arise that someone making the effort to visit that house intended to buy or to sell drugs there. *See, e.g., United States v. Long*, 678 F. App'x 31, 33 (2d Cir. 2017) (summary order); *United States v. Muhammad*, 520 F. App'x 31, 38 (2d Cir. 2013) (summary order). Questions then could arise about the scope of any search of that house or about the people who visited there. Here, there is no serious question that Playpen's primary purpose was to create an Internet community for child pornography and sexual exploitation of minors. If Playpen had been some kind of public site on the World Wide Web, and if visitors to a public site could be observed browsing the contents, then there would be no serious question about the presence of some kind of probable cause. Numerous courts around the country have wrestled with the unusual characteristics of the NIT, with varying results. The Court will not add to all of the ink spilled so far except to note that it has reviewed the developing case law and commends the parties for diligently bringing updates to its attention. And to be sure, the

Court had questions of its own while the case law was developing. The Court also expresses some displeasure at the details about the NIT that were missing from the search warrant that it issued. At a minimum, the Court would have asked more questions during the warrant application if it had known that a search of Sasiadek's house had been the culmination of an investigative technique that arguably amounted to malware and theoretically had international reach.

With all of that said, the Court now is aware that the Courts of Appeals have started to weigh in on the issues arising from the NIT. While the appellate courts in question do not yet include the Second Circuit, their analysis is persuasive and simplifies the challenge before this Court. These recent appellate opinions are particularly important because, with one critical exception at the end, they would eliminate the need for hearings and find for Sasiadek on every major substantive point. In *United States v. Horton*, 863 F.3d 1041 (8th Cir. 2017), the NIT helped FBI agents identify the defendant as a Playpen visitor under circumstances essentially identical to this case. The Eighth Circuit made a string of specific findings in favor of the defense. The Eighth Circuit found that "the execution of the NIT in this case required a warrant." *Id.* at 1047 (citation omitted). Next, the Eighth Circuit noted that Rule 41 does not allow "a magistrate judge in one jurisdiction to authorize the search of a computer in a different jurisdiction." *Id.*[4] The

[4] Though the timing has no impact on this case, the Court notes that Rule 41 underwent a significant amendment effective December 1, 2016. Under the amendment, "a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if . . . the district where the media or information is located has been concealed through technological means." Fed. R. Crim. P. 41(b)(6)(A). The notes accompanying the amendment specifically mention "anonymizing software" as a factor behind the change. Fed. R. Crim. P. 41(b)(6) Advisory Committee's note to 2016 amendment. "The amendment does not address constitutional questions, such as the specificity of description that the Fourth Amendment may require in a

Eighth Circuit concluded "that the NIT warrant exceeded the magistrate judge's jurisdiction." *Id.* at 1048. The Eighth Circuit even went as far as to state that "[w]e agree with the district court and find that the NIT warrant was void *ab initio*, rising to the level of a constitutional infirmity." *Id.* at 1049. Nonetheless, the Eighth Circuit found that suppression was not appropriate under *United States v. Leon*, 468 U.S. 897 (1984). The Eighth Circuit found that the NIT warrant application in the Eastern District of Virginia contained enough information that "a reasonable reader would have understood that the search would extend beyond the boundaries of the district because of the thorough explanation provided in the attached affidavit. This does not amount to a reckless disregard for the truth." *Id.* at 1052. The Eighth Circuit then reviewed the courts around the country that have considered the NIT warrant facially valid and the courts that have disagreed over the types of issues that Sasiadek raises here. The Eighth Circuit concluded that any error in issuing the NIT warrant belonged to the Magistrate Judge and not to the FBI agents, meaning that the deterrence benefits of suppression did not outweigh the cost to the criminal justice system. *See id.* On the sole basis of *Leon*, the Eighth Circuit reversed the District Court's suppression of evidence. The Tenth Circuit followed an abbreviated but similar analysis in its own NIT case: "For the sake of argument, we assume that (1) the magistrate judge in the Eastern District of Virginia lacked authority to issue the warrant and (2) the resulting search was unconstitutional or a prejudicial violation of federal law or a federal rule." *United States v. Workman*, 863 F.3d 1313,

---

warrant for remotely searching electronic storage media or seizing or copying electronically stored information, leaving the application of this and other constitutional standards to ongoing case law development." *Id.*

1317 (10th Cir. 2017) (citation omitted). The Tenth Circuit then reversed a suppression of evidence on the basis of *Leon*:

> We expect agents executing warrants to be 'reasonably well-trained,' but we do not expect them to understand legal nuances the way that an attorney would . . . . Thus, objective reasonableness sometimes turns on the clarity of existing law.
>
> For purposes of our discussion, we assume (without deciding) that the extraction of data from a user's computer in another district would violate the Federal Magistrates Act and the Federal Rules of Criminal Procedure. But if a violation took place, it has escaped the notice of eight federal judges who have held that the same warrant complied with federal law and the federal rules even though data was being extracted from computers outside the Eastern District of Virginia.
>
> These eight federal judges would have been mistaken if the warrant here were invalid. But executing agents could reasonably have made the same mistake and reasonably relied on the magistrate judge's decision to issue the warrant.

United States v. Workman, 863 F.3d 1313, 1321 (10th Cir. 2017) (citations omitted); *see also United States v. Levin*, ___ F.3d ___, No. 16-1567, 2017 WL 4855774, at *6 (1st Cir. Oct. 27, 2017) ("To the extent that a mistake was made in issuing the warrant, it was made by the magistrate judge, not by the executing officers, and the executing officers had no reason to suppose that a mistake had been made and the warrant was invalid. As discussed above, the NIT warrant was not written in general terms that would have signaled to a reasonable officer that something was amiss.").

This Court adopts *Horton*, *Workman*, and *Levin* as persuasive authority that eliminates the need for hearings. Under these cases, the Court is willing *arguendo* to grant Sasiadek every substantive point that he has raised: that the NIT warrant violated Rule 41; that the violation rose to a level of constitutional magnitude; and even that the NIT warrant was void *ab initio*. Nonetheless, despite the absence of some details that would have provided additional context, the NIT warrant application did give the Magistrate Judge in the Eastern District of Virginia some idea

as to its scope. The search warrant application for Sasiadek's residence similarly lacked some context but not critical information. With dozens of courts around the country wrestling with the intersection of Rule 41 and the new NIT technology, the Court hesitates to conclude that the FBI agents in question should have exercised a level of legal wisdom that has eluded the federal judiciary so far. To the extent that Sasiadek's arguments imply a policy question—when new technology creates a vacuum in legislative or regulatory guidance, is an *ex parte* application before a single duty judge the best way to fill that vacuum?—he has an extensive record in this case if he wants to pursue that question through the appellate or political processes.

IV. CONCLUSION

For all of the foregoing reasons, the Court respectfully recommends denying Sasiadek's motions to suppress. (Dkt. No. 30 at 3; Dkt. No. 87.)

V. OBJECTIONS

A copy of this Report and Recommendation will be sent to counsel for the parties by electronic filing on the date below. Any objections to this Report and Recommendation must be electronically filed with the Clerk of the Court within 14 days. *See* 28 U.S.C. § 636(b)(1); Fed. R. Crim. P. 59. "As a rule, a party's failure to object to any purported error or omission in a magistrate judge's report waives further judicial review of the point." *Cephas v. Nash*, 328 F.3d 98, 107 (2d Cir. 2003) (citations omitted).

SO ORDERED.

/s Hugh B. Scott

Hon. Hugh B. Scott
United States Magistrate Judge

DATED: November 2, 2017